

**IN THE UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF TENNESSEE
MEMPHIS DIVISION**

FREE SPEECH COALITION, INC.;
DEEP CONNECTION TECHNOLO-
GIES, INC.; JFF PUBLICATIONS, LLC;
PHE, INC.,; and MELROSE MICHAELS,

Case No. 2:24-cv-02933 (W.D. TN 2024)

Plaintiffs,

v.

JONATHAN SKRMETTI, in his official
capacity as the Attorney General of Tennes-
see,

Defendant.

DECLARATION OF TONY ALLEN

1. I, Tony Allen, am over the age of 18 and have personal knowledge of the facts set forth in this declaration. I have been retained by the State of Tennessee in *Free Speech Coalition, et al v Skrmetti*, No. 2:24-cv-02933 (W.D. TN 2024), to provide testimony on the systems, processes, and procedures that may be available to adult content providers to discharge their responsibilities under Tennessee’s SB 1792 (known as the “Protect Tennessee Minors Act” or “PTMA” and referred to in this declaration as “the Act”). This legislation implements acts to protect minors from viewing or accessing adult content online through amendments to Title 39, Chapter 17 and Title 47 of the Tennessee Code. By § 3, the Act comes into effect on January, 1 2025. The Act is not retrospective.

2. I am being compensated by the Office of the Attorney General of Tennessee. My compensation does not depend on the outcome of this litigation, the opinions I express, or the testimony I provide.

3. I have reviewed the Act; Plaintiff's complaint for declaratory and injunctive relief, motion for preliminary injunction, memorandum in support of its motion for preliminary injunction; and five declarations in support of Plaintiff's Motion: one from Andrea Barrica (dated November 20, 2024), Alison Boden (dated November, 26 2024), Chad Davis (dated November, 20 2024), Dominic Ford (dated November 20, 2024), and MelRose Michaels (dated November 26, 2024). I may wish to supplement my opinions or the bases for them as new evidence comes to light or new research is published.

4. I have nothing to add to or respond to the declarations of Andrew Barrica, Chad Davis or MelRose Michaels. I will comment on some of the content of the declaration of Alison Boden and briefly on that of Dominic Ford.

Personal Background

5. I am a Chartered Trading Standards Practitioner and Global Subject Matter Expert on Age Assurance Systems. I am the Technical Editor of ISO/IEC DIS 27566-1 – Information security, cybersecurity, and privacy protection – Age assurance systems – Part 1: Framework. I am the author of the book “Age Restricted Sales: The Law in England and Wales.”

6. I am also the Founder and Executive Director of the Age Check Certification Scheme, the leading UK Accreditation Service approved auditor and technology testing service for the age-assurance industry. I am also an audit member of the Age Verification Providers Association (“AVPA”)—a global trade association representing the age-assurance industry.

7. I have personal knowledge of the history, process, and logistics of online age assurance (as defined herein).

8. I have also been closely involved in the development of age-assurance legislation in the United Kingdom and elsewhere in the world, including the United States of America.

Summary

9. Tennessee's SB 1792 requires an individual or commercial entity that publishes or distributes in Tennessee a website that contains a substantial portion of content harmful to minors is liable if the individual or commercial entity does not:

- (a) Verify, using a reasonable age-verification method, the age of each active user attempting to access its website; or
- (b) Verify, using a reasonable age-verification method, the age of an active user attempting to access its website again after completion of an age-verified session.

10. This Act does not specify the manner in which age verification must be performed by stating that "Reasonable age-verification method" includes the following means of establishing the age of the person attempting to view content harmful to minors, implemented in a manner not easily bypassed or circumvented:

- (a) The matching of a photograph of the active user taken between the attempt to view content harmful to minors and the viewing of content harmful to minors, using the device by which the attempt to view content harmful to minors is being made, to the photograph on a valid form of identification issued by a state of the United States of America; or
- (b) A commercially reasonable method relying on public or private transactional data to verify that the age of the person attempting to access the information is at least eighteen (18) years of age or older;

11. Transactional data is further defined as a sequence of information that documents an exchange, agreement, or transfer between an individual, commercial entity, or third party used for the purpose of satisfying a request or event; and includes records from a mortgage, education, or employment.

12. Based on my knowledge and experience, modern technology is capable of allowing providers of adult content services to verify the ages of their consumers in a variety of ways, without jeopardizing either the providers' or consumers' interests in access or privacy.

13. The Act does not specify a required level of certainty, but does state that the age verification method should not be "easily bypassed or circumvented". We typically see levels of certainty in excess of 95%, usually around 99%.

14. Further, the burden and cost of verifying age is minimal and reducing every day as technology evolves ever more. Adult content companies already provide age-verification tools for the creation of accounts, to authorize the upload of content, or to verify the age of participants in video content (See Ford Decl. (Doc 2.4 ¶¶ 12). The prices described by Ford (Doc 2.4 ¶¶ 12-13) and Boden (Doc 2.2 ¶¶ 7), whilst within the bounds of possibility, are at the upper end of expectations and would tend to relate to full know-your-customer and anti-money laundering level checks. It is, of course, a matter for the market to respond to new demand created by the legislation, but elsewhere we see prices for simple age verification in the \$0.08 - \$0.15 range. In some cases, some for the kind of volumes listed by Boden (Doc 2.2 ¶¶ 7), the prices can be substantially discounted from headline or published rates by negotiation between the adult content provider and the age verification provider.

15. Based on my knowledge and experience, parental control features (See, e.g., Compl. (Doc. 1) ¶¶ 51), when properly installed, provide only a partial solution. The availability of these features are

further enhanced where the adult content provider is age aware of its users, so these technology stack level filters are less effective on their own than, and not a substitute for, website-based age assurance.

16. Many of FSC’s members already have tools to assist parents, and already have rules including the FSC Code of Ethics to “take all necessary precautions to prevent minors from viewing the adult content”. *See, e.g.*, Compl. (Doc. 1) ¶¶ 4.

Age Assurance Services

17. The Act requires adult content providers to verify the age of applicants before granting access to adult content. It gives some constraints, but does not dictate the precise processes or approaches on how to do that. I infer that the legislators assumed adult content providers would turn to the existing field of “age assurance”, as they have in other jurisdictions.

18. I am the Technical Editor of the International Standard on Age Assurance Systems, and extracts from those standards will help the Court understand what age assurance is.

19. I start with some definitions from ISO/IEC DIS 27566-1 – Age assurance systems – Part 1: Framework, clause 3:

“**Age assurance** is a set of processes and methods used to verify, estimate or infer the age or age range of an individual, enabling organizations to make age-related eligibility decisions with varying degrees of certainty.”

“An **age assurance result** is information produced by an age assurance system indicating that an individual is a certain age, over or under a certain age or within an age range.”

20. Age assurance is not a new or rare technology. It is widely used by thousands of sellers and their consumers on a daily basis around the world in various contexts, such as alcohol and tobacco sales, gambling, gaming, social media, and, to a growing extent, accessing pornography.

21. In April 2024, a Global Age Assurance Standards Summit was held in Manchester, UK, which generated a full compendium of the approaches to age assurance, the state of standards development,

and the latest state-of-the-art. *Compendium*, Global Age Assurance Standards Summit 2024 (Apr. 2024), (<https://accscheme.com/wp-content/uploads/ACCS-GlobalSummit-Compendium-.pdf>).

22. The Global Summit concluded with a consensus statement that:

- a. Age assurance **can** be done.
- b. Age assurance **can** be deployed, with the right process for the right use cases, in a manner that is privacy preserving, secure, effective, and efficient.
- c. Age assurance **can** be a valuable tool among a range of measures deployed to protect children in the digital environment.
- d. Age assurance is assisted by securing International Standards, which are implemented and respected by providers of services that are required to make age-related eligibility decisions.
- e. Laws and regulations **can** create the legal framework with robust enforcement procedures in place to secure the protection of children from harm.

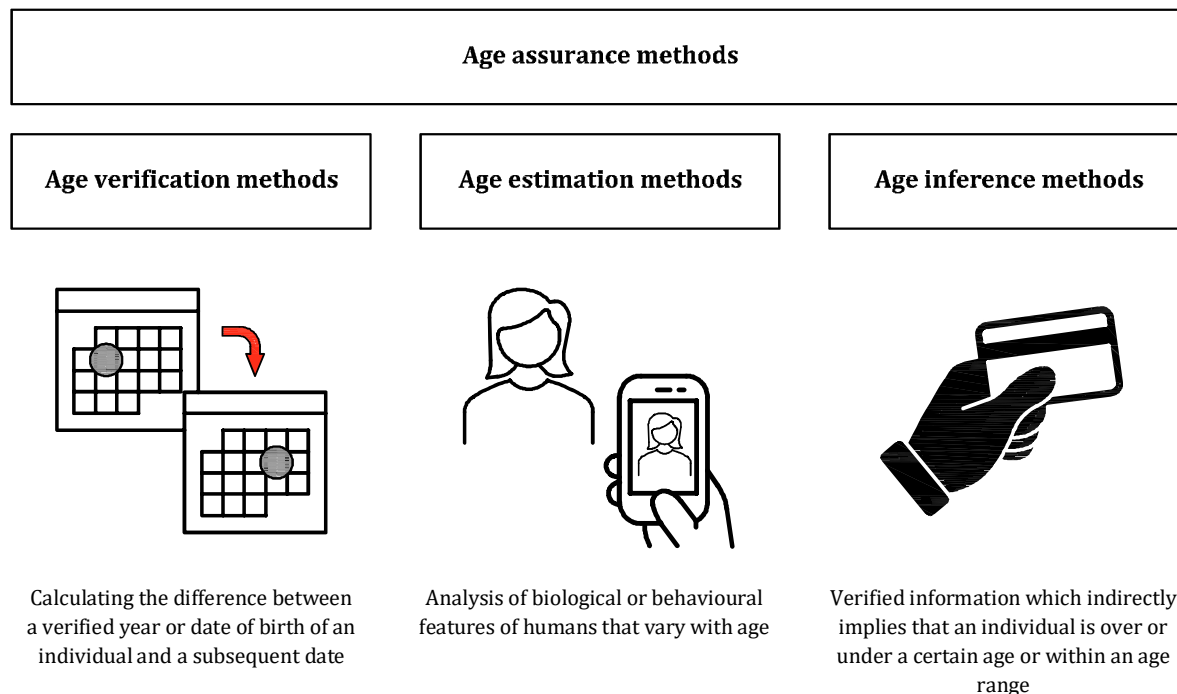
Communique, Global Age Assurance Standards Summit (Apr. 12, 2024), (<https://accscheme.com/wp-content/uploads/ACCS-GlobalSummit-Communique-FINAL.pdf>).

23. Further, third-party services continue to grow in number and improve the age-verification technology. The AVPA began in 2018 with just six members. It now has thirty members and there are at least forty providers competing in the global market.

24. A number of methods have been developed, initially to verify age exactly, and more recently, to estimate it with an ever-increasing degree of accuracy.

25. ISO/IEC DIS 27566-1 defines five core characteristics of age-assurance systems: functionality, performance, privacy, security, and acceptability. FSC's members could either develop their own age-assurance systems in accordance with the characteristics of ISO/IEC DIS 27566-1 or procure from the marketplace age-assurance systems that are built to those characteristics. I produce, as Annex 1, a copy of ISO/IEC DIS 27566-1 for the record.

26. ISO/IEC 27566-1 defines three different methods of age assurance:



27. The Act does not require adult content providers to establish the date of birth of the user, merely that they determine they are not a minor. Although the Act uses the term “verify,” the industry would not understand that term to mandate a specific age-assurance method, as age estimation and age inference are also suitable approaches to verifying an individual’s age-related eligibility.

28. In my opinion, the wording of the Act that

“anonymized age-verification data refers to data sufficient to prove a reasonable age-verification method was used to verify the age of the active user as eighteen (18) or more years of age and dissociated with any personally identifying information. At a minimum, anonymized age-verification data must include architectural diagrams illustrating the technological assets and logical processes by which the reasonable age-verification method is accomplished and data demonstrating a volume of reasonable age-verification method executions consistent with the overall volume of visits to the website”;

is sufficiently broad to include all three potential methodologies for age assurance.

The availability of age verification services and how they work

29. Age Verification in the context of the Act is the process by which the provider of internet content that is harmful to minors (“Adult Content Provider”) verifies that the consumer of the content is age 18 or older.

30. I am aware that age verification is already actively deployed by many adult content service providers including Dorcel, Only Fans, Jacqui & Michel, StripChat, PornHub, MyDirty Hobby, Clips4Sale, MYM, Skokka, Live Jasmin, FanCentro, Loyal Fans, Viva Street and xHamster, who are all subscribers to at least one Age Verification Provider, a company mentioned by the Boden (Doc 2.2 ¶¶ 7) called, Yoti (<https://www.yoti.com/>). These companies have applied age verification to one extent or another to their services elsewhere in the US, but also in the UK, France, Germany, Italy and in some cases, globally. PornHub have issued public information about their existing approaches to age verification (<https://www.pornhub.com/press/show?id=2172>).

31. Age verification began in rudimentary style, perhaps with a faxed copy of a driver's license, but is now far more sophisticated, far less expensive, and employs robust safeguards for privacy concerns.

32. With the explosion of pornography on the internet, representative governments, including multiple states in the United States and many countries around the world, have looked for ways to protect children from harmful content on the internet, while simultaneously protecting rights of speech and privacy. The goal is to create safer places online where children can enjoy and benefit from the opportunities created by the worldwide web (<https://ec.europa.eu/research/participants/documents/downloadPublic?documentIds=080166e5df252f14&appId=PPGMS>).

33. The market has developed privacy preserving Third-Party Services that provide straightforward solutions to carry out the age checks and then pass on only the outcome of those checks to the

sites a user wished to visit. The various data protection laws globally insist that providers only collect, process, and retain the data required for the specified purpose. So, generally where an Age Verification Provider obtained a consumer's personal information in order to confirm a user's age, it then had no further need to retain that data, and could delete it forthwith, storing only a user's account name, their age, and some form of password. This approach, therefore, does not require that all visitors to an adult website transmit to it their personal information and pre-empt any data breach.

34. In 2017, the UK government passed the Digital Economy Act which included a provision that sought to ensure that minors could not normally access pornography without age verification. Both consumers and the adult websites themselves expressed concerns about privacy – particularly the risk that a treasure trove database of users' identities connected to the adult websites they chose to visit would be exposed by hackers. So, from the outset, privacy was a primary objective for those designing technical solutions for the age verification.

35. Any question about whether an adult site is compliant with an age restricting law requires only a simple and straightforward audit of the verification process; no individual records or personal identifying information are needed.

36. When using an Age Verification Provider, an Adult Content Provider directs the consumer to provide personal information directly to the Age Verification Provider who performs the verification and informs the Adult Content Provider only of the result of the check – “pass” or “fail.” It does not pass back the personal information. This is usually in response to a binary question (is this user over 18?) to which the answer can only be ‘Yes’ or ‘No’. It is sometimes accompanied by a statement from the Age Verification Provider about how sure they are that their answer is correct

(say 99% or 99.9%). It should be noted that whilst this statement can be a very high percentage, it will never be 100%.

37. The Age Verification Provider does not generally retain a consumer's personal Information other than the date of birth, which can be used to respond to subsequent enquiries about that user's age.

38. The verification process need only be performed once per user and, as discussed further herein, the verification results for any individual user may be shared among Adult Content Providers and other websites, thereby minimizing the need for multiple age verification checks of the same individual.

39. Users may be asked to authenticate when they wish to re-use a previously completed age check. This is the process of confirming the same user who completed the check is the current user. It can be achieved simply with a password or Personal Identification Number (PIN) or for a higher level of assurance, a biometric interaction such as how users currently open their cell phone.

Methods of available age verification

40. A number of methods have been developed, initially to verify age exactly, and more recently, to estimate it with an ever-increasing degree of accuracy.

41. Previous implementations of Age Verification solutions, such as in France where consumers are offered a range of methods from which to choose, showed consumers vary in their preferences of Age Verification method. A choice of methods, rather than a single one, led to greater adoption of age verification.

42. A choice of methods also addresses issues that arise from inclusivity, should any one method not be suitable for an individual.

43. Age verification and age inference can be achieved by, among other methods, reference to drivers' licenses, passports, electoral rolls, credit reports, cellphone-network records, banking, and credit-card records. Users can also choose to create a digital identity and selectively release just their age attributes.

44. Age estimation, on the other hand, can be achieved by analyzing facial images, voiceprints, or other personalized evidence. The most advanced of these, facial estimation, is accurate to within ± 0.8 to 1.2 years mean absolute error, according to the latest published data by a certified age-assurance provider, Yoti Limited. *See Yoti Facial Age Estimation*, Yoti (Sept. 2024), <https://www.yoti.com/wp-content/uploads/2024/10/Yoti-Age-Estimation-White-Paper-September-2024-PUBLIC.pdf>. My certification team has independently verified and validated the results of Yoti's testing.

45. The value of age estimation for adult content providers and consumers is that it does not require consumers to submit any personal information other than a photograph or voiceprint, which is then instantly discarded. This system is already deployed for the purpose of verifying the age of users on social media site Instagram. *Introducing New Ways to Verify Age on Instagram*, Meta (June 23, 2022), (<https://about.fb.com/news/2022/06/new-ways-to-verify-age-on-instagram/>).

46. It is important to be clear from the outset that age-*estimation* technology is not *recognition* technology; it detects and assesses information, to give an age estimation, but it does not seek to identify who the person in the image or recording is. No image matching takes place for the purpose of estimating age.

47. A number of features and characteristics of people change with age. This allows for them to be analyzed to estimate age. An example of this is facial features. When facial age estimation is applied, users are either prompted to share a still or video image, or an existing profile picture can be used; and

software then estimates their age. Systems learn how to do this by reviewing thousands of images of people with a known age to spot patterns common to those of the same age, which means the technology is becoming better by the day. A live face is detected using liveness detection and then a pixel level review of the face is undertaken. The image generated by this method does not uniquely recognize any individual.

48. Although adult content providers can perform age assurance themselves, they can, and often do, contract with third-party companies to perform the service. An advantage of age estimation techniques is that they can be considerably cheaper, more privacy preserving and easier to implement than some age verification or age inference techniques.

49. The third-party service does not retain a consumer's personal information other than the date of birth, which can be used to respond to subsequent enquiries about that user's age. I have noted the requirement in the Act that website owner, commercial entity, or third party that executes a required age verification method shall:

- (a) Retain at least seven (7) years of historical anonymized age-verification data; and
- (b) Not retain any personally identifying information of the active user after access to the content harmful to minors has been granted.

50. In my experience independent, certified age assurance service providers are capable of complying with these requirements.

51. The verification process need only be performed once per user if they return "over 18", and the verification results for any individual user may be shared within the ecosystem of the adult content provider, thereby minimizing the need for multiple age-verification checks of the same individual. This can be accomplished by storing authenticated tokens or providing an account log in facility for users (as described by Ford Decl (Doc 2.4 ¶¶ 12-13).

52. Age assurance may be performed online from home or anywhere the user has access to the internet and can usually be completed in less than a minute. The production of ID documents is just one way to do age verification, it is not the most popular method; and, as a result, age-assurance systems have evolved that do not rely on this method.

53. There are a wide range of non-exclusive reasonable age verification methods that Content Providers and Third-Party Services can adopt to assure the ages of their users to varying degrees of certainty. These methods are used across the full range of situations where online age checks are required and have been certified by the Age Check Certification Scheme, which I manage.

54. Those which would be appropriate for implementing the Act include the following;

a. Review of Government Issued Documents

A reliable, physical identity document can be reviewed, and the age details noted. Users will typically submit an image of one or more of these documents using a smartphone camera. Technology, known as optical character recognition (OCR) reads the data from the document which is then validated based on known security features built into the form of ID used. The photo on the document can also be compared to a freshly taken photo or video of the user, which is known as a “liveness” check. For the highest levels of assurance Near Field Communication (NFC) technology can be used to allow a smartphone to read a microchip in the document where this is available, and the data on the chip compared to the image on the document, and a fresh photo or video of the user.

b. Review of Credit reports and other private sector databases

In this method, users typically enter their name, address, and date of birth (Either specifically for the purposes of age verification or as part of their account opening or purchase process for the website they wish to access), and a search is made of credit reports or other reliable databases to confirm the details are accurate and can obtain or confirm the date of birth. Often, this form of check is used

where the user will need to be located at the address claimed as part of this process, to prevent users entering the information of other people, so it is well suited to the delivery of age-restricted goods.

a. Review of digital identity apps

Digital identity apps or wallets are being certified in certain parts of the world, e.g., UK, Europe, Australia, Singapore - these approaches can enable citizens to share their over or underage status; via selective disclosure, in a data minimized way. Based on information and belief, I understand that Tennessee does not yet have a state issued digital identification card or app.

b. Submission of Credit Card number

In many countries, credit cards are only issued to adults, so the possession and the ability to use a credit card is a potential indicator that someone is over 18, but it is worth noting that this is not universal.

c. Review of bank records

Banks generally require a strong level of identification check to open an account, and keep a record of their customers' dates of birth. Some banks allow trusted third parties to confirm a date of birth supplied to them by the customer with those records. Typically, the user logs into their own online banking system, and gives approval for the data to be supplied to the third party, which in this case would be the Age Verification Provider.

d. Age estimation via facial, voice, or behavioral analysis

It is important to be clear from the outset that age *estimation* technology is not a *recognition* technology; it detects and assesses information, to give an age estimation. This is expanded on below with a particular focus on facial age estimation.

55. As stated above, facial age estimation is often falsely conflated with facial recognition technologies. In fact, the facial estimation technique described here is quite distinct from facial recognition. No image matching takes place for the purpose of estimating age.

56. Facial recognition may separately be used to check that a user relying on a previous age check is still the same individual who completed the check, but that is a separate process required for “authentication” rather than age estimation. Other estimation methods use voiceprints or analysis of how a user plays a computer game.

57. Presently, to meet a specific legal requirement for a person to be prevented from accessing material or services on the internet under a given age, increased confidence in the certainty of the age of a user of a site is possible by using systems that can be set with a “buffer” of an age level over and above the legally set age requirement. This approach will return a negative result if someone is estimated to be below the buffer age rather than below the legal threshold. The size of this buffer depends on the level of accuracy required by the Web service, or any regulatory requirements.

58. This method is inclusive of people of all ages, who do not own or have access to a government issued document. Age Estimation by facial or voice technology is one tool in a toolbelt. For example, for a law that requires a user to be aged 18 or older, such technology may be useful for assuring that individuals are, say, 21 years or older even if the Adult Content Provider and Age Verification Provider does not know their exact age. For those individuals, no further inquiry is needed. For those, however, whose facial or voice estimation results indicate an age range of under 21, then another Age Assurance method described herein may be used to confirm the exact age of the user.

59. Other methods of reasonable age verification, but which have not been subject to independent testing and certification, may include physical checks and vouching.

a. *Physical Check*

This is where a user is enrolled into an age assurance program in person. They may be asked to produce a physical proof of age which is checked by a trained member of staff, or it could be left to the judgement of staff to decide if someone looks at least 35, for example, who then certifies the user to be over 21.

b. Vouching

This is where other people with credibility are able to confirm a user's age. They may be professionals, such as teachers or doctors. It is one of the most inclusive methods of age verification, as users do not need to have any documents or particular records.

You can only vouch for someone if all of the following statements apply:

- i. you have an existing relationship with the user;
- ii. you are sure the user is who they say they are;
- iii. you are in a position of authority in their community; and
- iv. you have proved your own identity.

60. The Act allows for a wide range of the reasonable methods described above, giving users a choice that suits their own circumstances and preferences, and ensures accessibility by not narrowly defining acceptable methods which could then exclude certain groups e.g., those without government-issued ID documents.

61. There are other methods of age assurance that are less reliable than those previously discussed and, subject to the facts of any specific subsequent case, may not amount to reasonable age verification methods for the purpose of the Act.

62. An example is known as Attestation or Self-Declaration. This is not considered a method that provides any assurance about the user's age, but can provide a starting point for the process, and in some cases where there is no risk in believing the answer given is accurate, it may still be fit-

for-purpose. For example, if a child declares they are a child, then it may not be a problem to assume they are and protect them from harmful material on the internet. There are, however, sometimes good reasons to ensure children accessing websites on the internet are really children; for example, to prevent adults impersonating children online, so a more rigorous method is required.

63. Self-declaration is simply asking users to check a box, or enter their age or date of birth – without any additional checking against other data sources. Technical measures can improve reliability slightly – for example, allowing any year of birth to be entered, not only the year from before which the user would meet the site’s minimum age requirement, or preventing users applying trial and error by repeatedly amending their age until they are admitted.

64. These weak methods of age assurance would not, on their own, achieve the level of accuracy required for robust age verification, which satisfies the principal international standard for age checks. They can be used in combination with other age assurance techniques, which is why they are included in this summary, but on their own, they fall outside the scope of age assurance and the international standards the industry has developed.

Accuracy of methods, geolocation and circumvention

65. Each of these age verification methods, alone or in combination, verify age to a different level of certainty.

66. Regulators, or a regulated business, can determine this “level of assurance.” For example, regulators or regulated businesses might use different processes for alcohol sales, gambling, pornography access, and knife, gun or ammunitions purchases.

67. The plaintiffs express a concern that “minors can use virtual private networks (VPNs), proxy servers, the “Tor” browser, and numerous other circumventions to bypass the Act’s verification requirements with ease.” Many online services already block traffic from well-known VPNs. For

example, UK television channels the BBC and ITV actively prevent users from pretending to be in a different geographical location in order to access content they would otherwise be unable to view from their real location (“Potentially blocked up to 1M pirate viewers in the historic England v. Denmark Euro 2020 match” <https://www.geocomply.com/resources/case-study/itv-tackles-streaming-piracy-with-geoguard/>). The most common way to achieve this is to look out for a single internet protocol (IP) address which is generating significantly more traffic services that allow businesses to check if a user’s IP address is associated with a VPN or TOR (<https://focsec.com/>) as well as open-source lists to assist sites which wish to prevent the use of VPNs (https://github.com/X4BNet/lists_vpn/blob/main/ipv4.txt). Generally, only more expensive, premium VPN services offer each user a new and unique IP address which is harder to identify and block. These are considerably more expensive than the most widely used VPNs, making it harder for most minors to take advantage of their services.

68. The online gaming industry already makes extensive use of compliance services which require gaming operators to validate a customer’s location to prove that the customer is located in a state or jurisdiction which permits online betting and gaming. One of the leading geolocation compliance providers is GeoComply. The company is licensed by state gaming regulators and its technology is tested for accuracy and adherence to regulatory standards. GeoComply conducts up to 1 billion geolocation transactions monthly from apps installed on 400m devices worldwide which allow a user to prove where they really are located. The company "Collects geolocation signals from multiple sources, including: GPS, WiFi, GSM, browser/HTML5 and IP address" to verify location accuracy. Further, GeoComply technology detects the use of location “spoofing” software or other methods of location obfuscation as is required under various state laws and regulations

(https://cdn.geocomply.com/wp/app/uploads/20230518141903/GeoComply-Core_Brochure_Gaming.pdf).

69. Age verification providers have invested heavily in anti-spoofing technology. This includes a number of techniques intended to reduce circumvention or ‘spoofing’ of age verification systems, including:

a. Liveness detection is generally deployed to ensure that where a facial image is used for facial age estimation, or is required for comparison with the photograph supplied as part of a government-issued ID, it is of a live human being who is presently using the device through which the age check is being completed.

b. Fake or altered documents are detected using a wide range of techniques. For example, AU10TIX employs a dual-layered defense against fake or altered documents. The aim is to combat not just visible fraud but also professional, organized-crime level of manipulations that employ advanced tools and possibly insider-expertise. AU10TIX case-level detection goes forensic in detecting altered as well as “manufactured” fakes, while AU10TIX traffic-level detection is detecting professional attack behavior, even when document manipulations are well hidden.

c. The combination of case-level forensics and traffic-level detection has shown that the currently known fraud statistics do not reflect the actual magnitude of fraud activity, with more sophisticated fraud (such as one utilizing generative AI Deepfake) technology actually showing constant increase “thanks” to the increasing availability of off-the-shelf tools.

d. Stolen documents can be detected by checking against published lists of compromised identity documents.

70. In general, the objective of most legislation in this field has been to ensure that sexually explicit content is not normally accessible by minors. In other words, most children should be

prevented from seeing most adult content most of the time. Neither age verification nor age estimation techniques can guarantee 100 per cent accuracy, any more than staff in an adult bookstore are infallible when they check the age of their customers. But the technology is more than capable of preventing an adult website from giving access to children, as is the standard required in the Act.

Re-usability

71. Businesses can offer their users a wide-range of privacy-preserving methods to estimate their age to a level of assurance that is proportionate to the level of risk presented by a site. Once an age verification check has been completed for one site, it is technically possible to re-use the outcome of that same check across any other website through a network that enables interoperability across websites through cooperation between their age verification technology suppliers. Regulators, standards bodies, or the interoperability networks themselves may place limits on the duration for re-use.

72. This approach means the technology exists now to ensure that the Act does not threaten the principle of navigating seamlessly between many websites operated by unrelated entities. In effect, it asks users to take a small step, equivalent in the real world to wearing a seatbelt and using car seats, to protect children from online harm.

73. Historically, the Age Verification industry realized around 2020 that users may be willing to help a site assure their age if they wish to open an account that will last them a lifetime, but for sites they are just visiting temporarily, this could quickly become inconvenient and expensive. Recognizing this, the age verification industry has invested in delivering a mechanism that allows for the re-use of one age check across multiple websites.

74. A project was developed in six member states of the European Union, but has since opened up worldwide and includes major US companies to further develop the concept. The euCONSENT

project, funded by the European Commission, was a successful proof of concept where 2,000 individuals from five countries visited three age-restricted websites in turn, relying on a check completed at the first site to access the other two. The project is now being put into live operation in Europe, and a similar solution may be made available in the United States, as many states, including Tennessee, move to require age verification.

75. Users can choose to agree to accept a token on their device that merely indicates to websites they visit later that the user has already had their age verified, so these websites don't trouble the user again but instead ask the organization which did the first age check if this user meets their age condition. All this is done without sharing any identity details; nor is the user's age stored within the token to preserve their anonymity. As these are held locally on the device, there is no centralized 'honeypot' of data that could be the target of a hack (this is sometimes referred to as decentralized identity attributes). This significantly reduces the risk of data compromise at scale and, in any event, it only indicates that a user is over 18 and nothing about the reasons why they may have needed to prove that (it could be buying tobacco, gambling, gaming, car hire, accessing pornography or anything with an age-related eligibility criteria).

76. The age verification industry has developed reusable solutions and cooperated to develop and pilot interoperability so that age-assurance processes add little to no delay to a user's access to the internet, as their clients do not wish to drive any users away.

77. The convenience of interoperable and reusable age checks will avoid any problematic second-order effects. For example, this approach means that new websites and apps that users do not yet trust with their personal information need not ask them to provide it, as they will be able to rely on a check completed through a site that the user already trusts.

78. It is also important to highlight that adult content websites can be configured to recognize age attributes from certain age verification app wallets or data stores. These can sometimes be shared free of charge, including the Yoti app which is free for anyone sharing Over Age (e.g., Over 18). This is a one-time setup, taking 3-5 minutes, which can be created any time and thereafter re-used to share age or identity details, privately, with relying parties across multiple industries.

Adding the latest encryption techniques

79. In 2022, the French Data Protection Authority, published an article titled Online Age Verification: Balancing Privacy and the Protection of Minors, CNIL (Sept. 22, 2022), <http://bit.ly/3EB1ISN> [hereinafter CNIL Report].

80. The CNIL Report states:

a. "The CNIL also recommends, more generally, the use of a trusted independent third party to prevent the direct transmission of identifying data about the user to the site or application offering pornographic content. With its recommendations, the CNIL is pursuing the dual objective of preventing minors from viewing content that is inappropriate for their age, while minimizing the data collected on internet users by the publishers of pornographic sites."

b. "In order to preserve the trust between all of the stakeholders and a high level of data protection, the CNIL therefore recommends that sites subject to age verification requirements should not carry out age verification operations themselves but should rely on third-party solutions whose validity has been independently verified."

Age Verification around the world

81. The EU Better Internet for Kids Strategy mirrors the same desire as the Act: "Our vision is for age-appropriate digital services, with every child in Europe protected, empowered, and respected online, and no one left behind."

82. The UK Parliament passed the Online Safety Act in September 2023. This requires “highly effective” age verification or age estimation to prevent children from being exposed to “Primary Priority Content” on social media and adult sites. This content was initially defined as relating to suicide, self-harm, dieting and pornography. As when age verification was first developed at scale to prevent minors accessing adult websites, there remains a critical focus on designing a solution that protects the privacy and data security of users, because this latest Bill is focused on children whose personal data is particularly sensitive. Maintaining the anonymity of children is a core design principle for the age verification sector.

83. It is also worth looking at countries such as Germany, where over 100 age assurance approaches have been reviewed and approved by the KJM regulatory body (<https://www.kjm-online.de/aufsicht/technischer-jugendmedienschutz/unzulaessige-angebote/altersverifikationssysteme>). There is clearly a healthy eco system of age assurance approaches and methods and many global companies, including some of those association members of the Plaintiff, which are already deploying age assurance approaches in many parts of the world.

84. There are many examples of increasing requirements for age verification for access to adult content online which are all aligned with Tennessee’s legislation.

Cost of Age Assurance

85. The leading sector requiring robust age verification was initially online gambling. As an industry with a strong return per customer, it tolerated relatively high costs per age check, perhaps as much as a dollar each. Naturally, as the age-assurance industry grew, competition put downward pressure on pricing, and it halved relatively quickly. Age assurance is not advanced ID document verification or know-your-customer checks often used for anti-money laundering or counterterrorist financing

controls. These can be much more expensive—perhaps as much as two or three dollars—but are wholly unnecessary to demonstrate compliance with laws, like the Act, that merely require verification of age. Services will do that function (but will not necessarily guarantee that you are not subject to financial sanctions in the U.S.) at a considerably lower cost.

86. Alongside competitive pressures, underlying costs were also falling. The earliest age-verification methods almost all relied on accessing third-party databases, such as credit reports, for which there was a substantial cost per check. The more successful providers secured volume discounts but were still facing a high fixed cost base. Naturally, providers looked for cheaper ways to deliver their services, so they looked beyond credit reports to banking and telecoms where good quality data was available at a much lower cost, or even at no variable cost at all.

87. As a leader of an independent conformity assessment body, I cannot speak to the specific pricing offered by individual providers. But the UK Government published an Impact Assessment in 2022 for the Online Safety Bill (as it was at the time), which estimated the cost per check to be 12 cents (converted from pence), with a caveat that this cost is expected to continue to fall through innovation, competition, and interoperability. In the UK Government's most recent update (October 2024) preparing for (what is now) the Online Safety Act 2023, they now estimate that the cost could be as low as 0.8 cents per check (converted from pence). I am aware of providers who offer age verification at no cost to certain sectors as part of a wider digital-identity service.

The Security of Data

88. Age-assurance providers that are members of the AVPA, and thus sign up to its code of conduct, do not create new databases when conducting age checks. There are, of course, sectors such as online gambling where regulators require audit trails, but the industry's general practice is *not* to retain

any personal information after an age check is completed as would be required by this Act. These audited providers do not create new databases of personal data, nor track the behavior of individuals online.

89. During age-verification processes, age-verification providers apply the same degree of security you would expect in financial transactions.

90. Specifically, age-verification companies have a duty of care around the protection of personal data and demonstrate their adherence to this duty through various forms of certification (*e.g.*, ISO 27001, SOC2, Cyber Essentials, BSI PAS 1296, etc.) to ensure personal data is dealt with securely.

91. There is now a global standard in IEEE 2089.1 and an emerging global certification process under it. There is also considerable work progressing on ISO/IEC DIS 27566-1 – Age assurance systems – Part 1: Framework, which will form part of global certification of age-assurance systems.

92. Though age-verification providers share the same risk of attacks as a bank or healthcare provider, these risks are inherent to the internet, not unique to age verification. However, unlike banks and healthcare providers, age-verification providers hold considerably less valuable data, if any data at all, that would be useful to a hacker.

93. In addition to local laws, such as General Data Protection Regulations (“GDPR”) in the UK and European Union, there is an industry-wide certification protocol, operated by government-approved auditors, which tests providers against international standards. This not only assesses the efficacy of the age check, but also data-security and privacy measures. Adult content providers governed by the Act may choose to use commercially available age-verification providers certified by these regulatory bodies, not only to consolidate their defense against potential legal claims but also to build consumer trust and confidence.

Ineffectiveness of Other Methods

94. Other existing methods for protecting children on the internet, including parental controls and web-filtering technology, are not mutually exclusive with age assurance. For example, both content filtering and age verification could be deployed consecutively or concurrently. Content filtering, however, has flaws and is no substitute for age verification and parental consent.

95. A neutral analysis of content filtering can be found in a report for the European Parliament's Policy Department for Citizens' Rights and Constitutional Affairs. *The Impact of Algorithms for Online Content Filtering or Moderation*, European Parliament (Sept. 2020), bit.ly/3A6jKNK.

96. Filtering applied in the home, on the router or on laptops, tablets, and smartphones, is generally managed by parents. We know from repeated research by the UK's telecom's regulator, OFCOM, that many parents are unaware of this technology. And those aware of it often do not know how to use it, or discover their children also know how to use it and circumvent it. And those who know about it and how to use it must still choose to use it. "Just over a quarter of parents used content filters provided by their broadband supplier, where the filters apply to all devices using that service (27%). A much larger proportion (61%) said they were aware of this feature, showing that not all parents are adopting this potentially useful control." *Children and Parents: Media Use and Attitudes Report 2022*, OFCOM (Mar. 30, 2022), https://www.ofcom.org.uk/__data/assets/pdf_file/0024/234609/childrens-media-use-and-attitudes-report-2022.pdf. A survey of U.S. parents by Kaspersky in 2021 found just 50% used any kind of parental controls. *See Study Finds 50% of Parents Use Parental Control Apps*, Kaspersky (Dec. 2, 2021), (https://usa.kaspersky.com/about/press-releases/2021_study-finds-50-of-parents-use-parental-control-apps).

97. Directions on how to circumvent parental controls are easily available on the internet, and children are succeeding at getting around parental-control features. *See, e.g.,* Yoree Koh, *Tech-Savvy Kids Defeat Apple's and Others' Parental-Control Features*, Wall St. J. (Dec. 19, 2021), on.wsj.com/3C7MciL.

98. Some parents describe supervising the children's internet usage as "a full-time job," *id.*, and that they are losing the "technological arms race over parental controls in the home," Stephen Johnson, *How Your Kids Are Outsmarting All Your Parental Controls*, Lifehacker (Dec. 21, 2021), <https://lifehacker.com/how-your-kids-are-outsmarting-all-your-parental-control-1848249586>.

99. Children today are adept at leveraging technological tools and exploiting system vulnerabilities to bypass parental controls. Here is an overview of the main strategies employed across various levels of restrictions:

100. Device-level restrictions, such as parental controls or default operating system settings, aim to limit access to inappropriate content or apps. However, children often circumvent these through:

- a. Factory resetting the device to remove parental control settings. Android and Apple devices both deactivate the parental control settings if the device is reset (Apple say this can be stopped by enabling Activation Lock in the Find My feature) (<https://discussions.apple.com/thread/253247939>).
- b. Creating secondary or "ghost" accounts without restrictions to access unrestricted content (<https://www.parentingwithfocus.org/post/the-complete-guide-to-parental-controls>).
- c. Using shared payment methods or family accounts to bypass content filters or download restricted apps.

- d. Gaining administrative control to remove restrictions set by manufacturers or guardians – this is sometimes called ‘jailbreaking’.

101. Network-Based Restrictions, such as firewalls or DNS-based filtering, are implemented to block inappropriate websites across devices connected to the network. Children bypass these using:

- a. Masking their location and bypassing content filtering through encrypted connections, such as the use of virtual private networks.
- b. Accessing restricted content through publicly available proxy sites. It is not impossible to identify these services (they have been blocked for the purpose of content licensing by the likes of Netflix, news sites and subscription TV channels)
- c. Connecting to unrestricted networks, such as mobile data, public Wi-Fi, or a friend's hotspot (the phenomenon of hotspot sharing in schools for popularity, means that pupils with less attentive parents to their online browsing can offer connection for other pupils where parents have set up controls).

102. Browser-Level Restrictions such as safe search configurations, or extensions aim to restrict access to adult or harmful content. Common circumvention tactics include:

- a. Downloading browsers that do not enforce the same restrictions or limitations (such as the Opera (<https://www.opera.com/>) which has built in tools to avoid restrictions.
- b. Avoiding detection and restrictions by using modes that do not save browsing history such as Incognito Mode (<https://support.google.com/chrome/answer/95464>).
- c. Removing evidence of blocked sites or attempts to bypass filters.
- d. Manipulating URLs to access content without triggering keyword-based restrictions.

103. Applications often include built-in self-declaration tools to limit access to certain features or content. Children evade these using:

- a. Entering incorrect birthdates to meet the minimum age requirements for apps or services - A third of children claim to be 18 or older on social media, and 22% of 8–17 year olds lie about their age on social media apps (<https://www.ofcom.org.uk/online-safety/protecting-children/a-third-of-children-have-false-social-media-age-of-18/>)
- b. Using adult or older sibling accounts to access restricted content.
- c. Downloading unauthorized versions of applications (called cracked apps) without restrictions from third-party app stores.
- d. Using exploits, such as trial resets or in-app loopholes, to access restricted content without parental approval.

104. These attack vectors can be applicable to age assurance systems too, however, where the age assurance process is conducted by specialist third party age verification providers, their systems are developed and designed to recognize these attack vectors and mitigate them. Children's ability to circumvent restrictions underscores the need for a multi-layered approach that combines technical solutions with active parental involvement and education. Solutions that evolve with technological advancements and incorporate behavioral insights can better address these challenges. As age assurance has technologically evolved over the last few years, its role in the holistic protection of children from online harm has become more paramount.

105. Research for the Federal Trade Commission (https://www.ftc.gov/system/files/documents/public_events/1582978/betrayed_by_the_guardian_-_security_and_privacy_risk_of_parental_control_solutions.pdf) examines the Security and Privacy Risks of Parental Control Solutions. The report concludes that:

“Our cross-platform comprehensive analysis of popular solutions shows systematic problems in the design and deployment of all the analyzed solutions (with some exceptions) from a security and privacy point of view. Indeed several of these solutions can undermine children’s online and real-world safety. As these solutions are viewed as an essential instrument to provide children a safer online experience by many parents, these solutions should be subjected to more rigorous and systematic evaluation, and more stringent regulations.”

106. Content-filtering software often over-blocks, preventing access to educational, informative, or harmless content. This can limit children’s learning opportunities and access to useful resources.

107. Filtering software is also an imperfect solution. Despite advancements, many filters fail to block all harmful content, allowing some inappropriate material to slip through. And many filtering tools collect data on browsing habits. This information can be mishandled or accessed by unauthorized parties. The privacy-infringement concerns raised about age verification also apply to content filtering. Research on Internet Filtering and Adolescent Exposure to Online Sexual Material concluded that caregiver’s use of internet filtering had inconsistent and practically insignificant links with young people’s reports of encountering sexual material online. Przybylski & Nash, *Cyberpsychol Behav Soc Netw.* 2018 Jul 1;21(7):405-10, (<https://www.ncbi.nlm.nih.gov/pmc/articles/PMC6101267/>)

108. Filtering software can reflect the biases of its developers, resulting in the blocking of content based on cultural or ideological standards that may not align with the values of all users. Overzealous filtering can infringe on children’s rights to access diverse viewpoints and information, which is essential for developing critical thinking skills and understanding the world.

109. The dynamic nature of the internet requires constant updates to filtering algorithms to keep up with new websites and changing content. This maintenance is resource-intensive and often

lags behind the creation of new harmful content. Filtering software can cause compatibility problems with other applications and devices, leading to a frustrating user experience.

110. High-quality filtering software can be expensive, typically in the range of \$4-5 per month per license.

111. Relying solely on content-filtering software can lead to complacency among parents and guardians, who mistakenly believe that the software provides complete protection. This can result in a lack of active engagement and communication with children about safe online behaviors.

112. Content filtering is not a replacement for what the Act requires of adult content providers for age verification. In short, content filtering is a less effective approach than the one the Act adopts.

113. Notably, FSC and its members resist laws requiring content filtering (or solutions like it), arguing that they violate U.S. federal law. *See, e.g., Computer & Comm'n's Indus. Ass'n (CCLIA) v. Paxton*, 2024 WL 4051786 (W.D. Tex. Aug. 30) (monitoring and filtering); *NetChoice, LLC v. Fitch*, 2024 WL 3276409 (S.D. Miss. July 1) (“commercially reasonable efforts to develop and implement a strategy to prevent or mitigate the known minor’s exposure to harmful material and other content that promotes or facilitates the following harms to minors”).

Parental Consent

114. Parental consent is generally done separately from age assurance or verification. This process generally occurs after an age-assurance process determines that a user is a minor.

115. There are numerous commercial providers of parental-consent services in the United States through the Children’s Online Privacy Protection Act (COPPA) Safe Harbor Program. *See*

COPPA Safe Harbor Program, Federal Trade Comm’n (last accessed Oct. 30, 2024), <https://www.ftc.gov/enforcement/coppa-safe-harbor-program>.

116. In implementing COPPA, the Federal Trade Commission set up a process that enables industry groups to seek safe harbor for how they gain parental consent. The list of currently approved Safe Harbor organizations is:

- Children’s Advertising Review Unit (CARU)
- Entertainment Software Rating Board (ESRB)
- iKeepSafe
- kidSAFE
- Privacy Vaults Online, Inc. (d/b/a PRIVO)
- TRUSTe

117. There are many methods of verifying parental consent, including:

- a. Email Verification: This is one of the simplest methods, where a parent receives an email requesting consent and must respond or click a link to confirm.
- b. Knowledge-Based Authentication: Here, the parent answers questions only they are likely to know, such as financial or historical details, which are verified against public records.
- c. Credit Card or Payment Verification: Many systems verify parental consent by requiring a small charge (often refundable) on a parent’s credit card. This method leverages the fact that payment cards are usually only available to adults.
- d. Government ID Verification: This method asks parents to upload a scanned ID (such as a driver’s license) for identity verification.
- e. Video Verification: In this approach, parents participate in a live video verification or upload a short video of themselves providing consent. This method can be reliable, especially if paired with AI for identity matching.
- f. Third-Party Verification Services: Some companies use third-party age-assurance providers specializing in parental-consent verification. These services manage verification across various methods (such as ID verification, payment, or biometric

checks), and ensure compliance with data protection and privacy laws like GDPR and COPPA.

What We've Learned

118. Age-assurance methods do not necessarily add a new step to a user's visit to a new website or app because, through re-usability and interoperability, one age check can be used across multiple sites seamlessly.

119. Some online services, including adult content providers, are already using age-assurance technology in some contexts. For example:

- a. Meta has deployed age-assurance measures on Instagram, using Yoti as a provider. *See Introducing New Ways to Verify Age on Instagram*, Meta (June 23, 2022), <https://about.fb.com/news/2022/06/new-ways-to-verify-age-on-instagram/>.
- b. TikTok scans public videos of users to help determine account holders' ages. *See Sarah Perez, TikTok CEO Says Company Scans Public Videos to Determine Users' Ages*, TechCrunch (Mar. 23, 2023), <https://techcrunch.com/2023/03/23/tiktok-ceo-says-company-scans-public-videos-to-determine-users-ages/>.
- c. Google's YouTube Official Blog states, "If our systems are unable to establish that a viewer is above the age of 18, we will request that they provide a valid ID or credit card to verify their age. We've built our age-verification process in keeping with Google's Privacy and Security Principles." *Using Technology to More Consistently Apply Age Restrictions*, YouTube Official Blog (Sept. 22, 2020), <https://blog.youtube/news-and-events/using-technology-more-consistently-apply-age-restrictions/>.
- d. If a user tries to change their self-reported age or has been identified as being underage, platforms, including Pinterest, Discord, TikTok, and Google, require users to verify their age with a government-issued ID, credit card, or a live photo.
- e. PlayStation has deployed age-assurance measures with Yoti. *Age Verification Frequently Asked Questions*, PlayStation (last accessed Oct. 29, 2024), <https://www.playstation.com/en-gb/support/account/age-verification-faq/#:~:text=Age%20verification%20allows%20us%20to,by%20our%20service%20provider%2C%20Yoti.>
- f. Age assurance is also now available on adult content websites through services like VerifyMy. *VerifyMyAge*, VerifyMy (last accessed Oct. 29, 2024), <https://verifymy.io/>.

120. Over the past 25 years, the age-verification industry has developed a wider range of ways to verify age that offer users choice, including alternatives to document-based approaches. Users can choose, for example, age-estimation techniques, which do not require ownership or use of a document and where the image is instantly deleted. Many hundreds of millions of age-assurance checks are now undertaken globally each year. The cost has dropped dramatically, with reusability likely to lead to that trend continuing so there are no undue burdens on adult content providers due to the high costs of implementing full ID-document and know-your-customer level verification technologies. Nor would there necessarily be any significant loss of traffic resulting from the use of these technologies, except, of course, from minors.

121. The UK Government estimate in the Impact Assessment for the Online Safety Act 2023 puts the cost per check at 12 cents and possibly as low as 0.8 cents for high volume platforms, but notes that the cost may reduce further through interoperability and growing competition. Those 12 cents also may be defrayed across 100 websites before the check needs to be repeated to maintain the ongoing integrity of the age-verification ecosystem, and that is only if businesses determine that periodic re-validation is prudent.

122. Concerns about anonymity have also been addressed. The age-verification sector was created specifically to enable users to access the sites they wished to access through the data-minimized sharing of age. By selecting a trusted third party, even when selective disclosure from full identity documents or a digital-identity wallet is used to prove age, the provider then only confirms “yes” or “no” when a website enquires “is this user an adult?” In Europe, users are given further reassurance by the enforcement of the General Data Protection Regulations; but in the United States, contractual commitments to maintain secrecy and the threat of civil damages claims if that is not applied offer similar protection. Also, age-assurance standards allow for vouching where a user with no

documentary proof of age can ask a respected member of their community, such as a teacher or doctor, to confirm their age.

123. Whether or not privacy laws apply, globally AVPA members must adhere to a Code of Conduct that requires privacy and data security. (*See Code of Conduct*, Age Verification Provider's Ass'n, <https://avpassociation.com/membership/avpa-code-of-conduct/>).

Pursuant to 28 U.S.C. §1746, I declare under penalty of perjury that the above statements are true and based on my personal knowledge.

ENDS

Executed December 16, 2024

Tony Allen
Tony Allen (Dec 16, 2024 20:53 GMT)

Tony Allen






2024.12.15 Allen Declaration Draft

Final Audit Report

2024-12-16

Created:	2024-12-16
By:	Tony Allen (tony.allen@accscheme.org.uk)
Status:	Signed
Transaction ID:	CBJCHBCAABAAAdNaa4xp3PJGgD-qvNucSIBjHURT2jLW_

"2024.12.15 Allen Declaration Draft" History

-  Document created by Tony Allen (tony.allen@accscheme.org.uk)
2024-12-16 - 8:52:33 PM GMT
-  Document emailed to Tony Allen (tony.allen@solicab.com) for signature
2024-12-16 - 8:52:39 PM GMT
-  Email viewed by Tony Allen (tony.allen@solicab.com)
2024-12-16 - 8:53:09 PM GMT
-  Document e-signed by Tony Allen (tony.allen@solicab.com)
Signature Date: 2024-12-16 - 8:53:41 PM GMT - Time Source: server
-  Agreement completed.
2024-12-16 - 8:53:41 PM GMT